UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/061,415	02/01/2002	Davide Libenzi	NAI1P393/01.162.01	9282

28875 7590 08/31/2007
Zilka-Kotab, PC
P.O. BOX 721120
SAN JOSE, CA 95172-1120

EXAMINER	
HENNING, MATTHEW T	
ART UNIT	PAPER NUMBER
2131	
MAIL DATE	DELIVERY MODE
08/31/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/061,415	**Applicant(s)** LIBENZI ET AL.	
	Examiner Matthew T. Henning	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *12 July 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-10,13-25,28-38,40-47 and 49-55* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-10,13-25,28-38,40-47 and 49-55* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *01 February 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

This action is in response to the communication filed on 7/12/2007.

DETAILED ACTION

Claims 1-10, 13-25, 28-38, 40-47, and 49-55 have been examined.

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114 was filed in this application after a decision by the Board of Patent Appeals and Interferences, but before the filing of a Notice of Appeal to the Court of Appeals for the Federal Circuit or the commencement of a civil action. Since this application is eligible for continued examination under 37 CFR 1.114 and the fee set forth in 37 CFR 1.17(e) has been timely paid, the appeal has been withdrawn pursuant to 37 CFR 1.114 and prosecution in this application has been reopened pursuant to 37 CFR 1.114. Applicant's submission filed on 7/12/2007 has been entered.

Specification

The disclosure is objected to because it contains an embedded hyperlink and/or other form of browser-executable code. Applicant is required to delete the embedded hyperlink and/or other form of browser-executable code. (See the specification Page 2 Line 1). See MPEP § 608.01.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-3, 5-10, 13-14, 16-18, 20-25, 28-29, 31 and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka et al. (US Patent Number 6,453,345) hereinafter referred to as Trcka, and further in view of Stevens (TCP/IP Illustrated).

Regarding claims 1, 16, and 31, Trcka disclosed a system for providing passive screening of transient messages in a distributed computing environment (See Trcka Abstract), comprising: a network interface (See Trcka Fig. 1 Element 38) passively monitoring a transient packet stream in a network boundary (See Trcka Col. 2 Lines 11-22) comprising receiving incoming datagrams structured in compliance with a network protocol layer (See Trcka Col. 2 Lines 23-24); an antivirus scanner scanning contents of the packets for a presence of at least one of a computer virus and malware to identify infected message contents (See Trcka Col. 3 Line 66 – Col. 4 Line 16); and a protocol specific module processing each packet based on the protocols employed by the packet (See Trcka Col. 13 Lines 32-49), but Trcka failed to specifically disclose a packet receiver reassembling one or more of the incoming datagrams into a segment structured in compliance with a transport protocol layer; or that the protocol specific module processed the reassembled datagrams based on the transport protocol layer employed by the reassembled datagram. However, Trcka did disclose performing virus scanning on specific upper layer files such as FTP, HTTP, SMTP, and others (See Trcka Col. 14 Lines 62-67).

It was well known that in the Internet Protocol there are multiple layers and that each layer contains different modules, such as the TCP module and the UDP module of the transport layer. It was also well known that in order to get to the data in the application layer packet, such as the payload and the packet type, the transport layer module must process the transport layer packet to reveal the application layer packet. This is evidenced by Stevens Pages 6-11.

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known in the art of networking and TCP/IP in order to gain access to the data in the packets for scanning, by demultiplexing (reassembling) the incoming Ethernet frames into IP packets, and then demultiplexing the IP packets into the proper transport layer segments according to the proper protocols in order to extract the data from the packets. This would have been obvious because the ordinary person skilled in the art would have been motivated to use what was common and well known in the art.

Regarding claims 2 and 17, Trcka and Stevens disclosed an incoming queue staging each incoming datagram intermediate to reassembly (See Trcka Col. 4 Line 8-10).

Regarding claims 3 and 18, Trcka and Stevens disclosed a network protocol-specific decoder decoding the reassembled segment prior to scanning (See Stevens Page 11 and the rejection of claim 1 above).

Regarding claims 5-6 and 20-21, Trcka and Stevens disclosed the antivirus scanner takes an action if the reassembled segment is infected with at least one of a computer virus and malware, wherein the action comprises at least one of logging an infection; generating a warning; spoofing a valid datagram in place of the infected datagram; and acquiescing to the infection (See Trcka Col. 13 Lines 1-15).

Regarding claims 7-10 and 22-25, Trcka and Stevens disclosed a protocol-specific queue staging each reassembled segment with other reassembled segments sharing the same transport protocol layer (See Trcka Col. 17 Line 56 – Col. 18 Line 14, Col. 19 Lines 55-59 and Col. 20 Lines 30-35), an information record storing information dependent on the same transport protocol layer with the staged reassembled segment (See Trcka Col. 12 Lines 7-11 and Col. 20

Lines 34-35), a contents record storing the contents with the staged reassembled segment (See Trcka Col. 18 Lines 15-52), and wherein the information comprises at least one of a source address, source port number, destination address, destination port number, URL, file name, user name, sender identification, recipient identification, and subject (See Trcka Col. 18 Lines 3-14). Furthermore, in the demultiplexing taught by Stevens, it would be obvious for each "protocol box" which is receiving data and acting on the, to have a queue for storing the data before and during the processing of this protocol specific data. This would be obvious because the ordinary person skilled in the art would have been motivated to not lose the data if a "protocol box" is processing data slower than it is receiving the data.

Regarding claims 13-14, and 28-29, Trcka and Stevens disclosed an event correlator analyzing the transient packet stream for events indicative of a network service attack (See Trcka Abstract and Col. 13 Lines 5-15), and a data repository maintaining each event (See Trcka Col. 7 Lines 28-32).

Regarding claim 55, Trcka and Stevens disclosed that the incoming datagrams include IP datagrams that are reassembled into TCP segments (See Trcka Col. 14 Lines 61-67).

Claims 4, 19, 32-38, 40-47, and 49-52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka and Stevens as applied to claim 1 above, and further in view of Cheriton (US Patent Number 7,054,930).

Trcka and Stevens disclose detecting and responding to network attacks (See Trcka Col. 11 Lines 14), but failed to specifically disclose detection or response to Denial of Service attacks, or terminating the transient packet stream if the reassembled segment is not infected with at least one of a computer virus and malware.

Cheriton teaches that in a network, denial of service attacks can result in significant loss of time and money for many organizations (See Cheriton Col. 1 Lines 19-21), and further teaches detection of denial of service attacks (See Cheriton Col. 3 Lines 29-45) and teaches generation and refinement of filters for stopping the attack packets, and forwarding these filters upstream (See Cheriton Col. 2 Lines 16-24 and Col. 3 Lines 29-45, and Claim 7).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Cheriton in the network surveillance system of Trcka and Stevens by detecting Denial of Service attacks, and upon detection of such, creating a filter to prevent the flow of the Denial of Service packets, and forwarding the filter for use by an upstream device. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to protect the network from Denial of Service attacks.

Regarding claims 32, 41, and 50, Trcka and Stevens disclosed a system for passively detecting computer viruses and malware and network attacks in a distributed computing environment (See Trcka Abstract), comprising: a network interface receiving copies of datagrams transiting a boundary of a network domain into an incoming packet queue (See Trcka Col. 2 Lines 29-34, Col. 4 Lines 2-11, and Col. 7 Lines 28-32, and Col. 12 Lines 29-40), each datagram being copied from a packet stream (See Trcka Col. 14 Lines 34-36); a packet receiver reassembling one or more such datagrams from the incoming packet queue into network protocol packets, each staged in a reassembled packet queue (See Stevens Pages 4-11 and the rejection of claim 1 above); an antivirus scanner scanning each network protocol packet from the reassembled packet queue to ascertain an infection of at least one of a computer virus and malware (See Trcka Col. 3 Line 66 – Col. 4 Line 16) ; and an event correlator evaluating events identified from the datagrams in the packet stream to detect network attack on the network domain (See Trcka Abstract and Col. 13 Lines 5-15) ; wherein a protocol-specific module processes each reassembled datagram, based on an upper protocol layer employed by the reassembled datagram (See Stevens Page 11 and the rejection of claim 1 above), but Trcka and Stevens failed to specifically disclose detection of Denial of Service type network attacks.

Cheriton teaches that in a network, denial of service attacks can result in significant loss of time and money for many organizations (See Cheriton Col. 1 Lines 19-21), and further teaches detection of denial of service attacks (See Cheriton Col. 3 Lines 29-45) and teaches generation and refinement of filters for stopping the attack packets, and forwarding these filters upstream (See Cheriton Col. 2 Lines 16-24 and Col. 3 Lines 29-45, and Claim 7).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Cheriton in the network surveillance system of Trcka and Stevens by detecting Denial of Service attacks, and upon detection of such, creating a filter to prevent the flow of the Denial of Service packets, and forwarding the filter for use by an upstream device. This would have been obvious because the ordinary person skilled in the art at the time of invention would have been motivated to protect the network from Denial of Service attacks.

Regarding claims 33 and 42, Trcka, Stevens and Cheriton disclosed a parser parsing each reassembled datagram into network protocol-specific information and packet content (See Stevens Page 11).

Regarding claims 34 and 43, Trcka, Stevens and Cheriton disclosed extracting the header information from the packets (See the rejection of claim 33 above), but failed to disclose specifically what information was contained in the headers. It was well known in the art at the time of invention that the headers of HTTP messages contained a source address and port number, a destination address and port number, and a URL, the headers of an FTP message contained the filename and username, and the headers for the SMTP contained the sender identifier, receiver identifier, and subject. As such, it would have been obvious to the ordinary person skilled in the art at the time of invention to employ what was well known by extracting the header information from the headers of the packets. This would have been obvious because the ordinary person would have been motivated to extract what was known to be contained in the header.

Regarding claims 35 and 44, Trcka, Stevens, and Cheriton disclosed a decoder decoding the packet content prior to performing the operation of scanning (See Stevens Page 11 and the rejection of claim 1 above).

Regarding claims 36 and 45, Trcka, Stevens, and Cheriton disclosed a log logging an occurrence of at least one of the infection and the network attack (See Trcka Col. 17 Lines 38-40).

Regarding claims 37, and 46, Trcka, Stevens, and Cheriton disclosed a warning module generating a warning responsive to an occurrence of at least one of the infection and the network attack (See Trcka Col. 13 Lines 1-15).

Regarding claims 38 and 47, Trcka, Stevens, and Cheriton disclosed a spoof module sending a spoofed network protocol packet responsive to an occurrence of at least one of the infection and network attack (See Cheriton col. 10 Line 41- Col. 11 Line 8 and Trcka Col. 17 Lines 37-39, wherein it would have been obvious to the ordinary person skilled in the art to send the detected spoofed packet to the log).

Regarding claim 51, Trcka, Stevens, and Cheriton disclosed that the network protocol packets employ at least one of F[TTP, F'I'P, SMTP, POP3, NNTP, and Gnutella network protocols (See Trcka Col. 18 Paragraphs 1-2).

Regarding claim 52, Trcka, Stevens, and Cheriton disclosed that only datagrams compliant with IP protocol are reassembled (See Trcka Entire reference wherein only IP compliant protocols are disclosed).

Claims 15, and 30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka and Stevens as applied to claims 1 and 16 above, and further in view of Hailpern et al. (US Patent Number 6,275,937) hereinafter referred to as Hailpern.

Trcka and Stevens disclosed a system for scanning IP network packets for viruses (See the rejection of claim 1 above), but failed to disclose that all the incoming messages were SMTP compliant, and therefore TCP compliant.

Hailpern teaches that virus scanning should be set up for each network protocol proxy, including E-mail, in order to scan for viruses (See Hailpern Col. 4 Lines 1-13).

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Hailpern in the virus scanning system of Trcka and Stevens by modifying mail servers to contain the scanning system of Trcka and Stevens. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the proxies to be able to scan the types of communications they already process and therefore reduce network traffic and delay. Further, SMTP mail servers were well known in the art at the time of invention, and it would have been obvious to utilize the scanning system of Trcka and Stevens in an SMTP mail server. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect SMTP mail servers from viruses.

Claims 40, 49, and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka and Stevens and Cheriton as applied to claims 32 and 41 above, and further in view of Hailpern et al. (US Patent Number 6,275,937) hereinafter referred to as Hailpern.

Trcka, Stevens, and Cheriton disclosed a system for scanning IP network packets for viruses (See the rejection of claim 1 above), but failed to disclose that all the incoming messages were SMTP compliant, and therefore TCP/IP compliant.

Hailpern teaches that virus scanning should be set up for each network protocol proxy, including E-mail, in order to scan for viruses (See Hailpern Col. 4 Lines 1-13).

It would have been obvious to the ordinary person skilled in the art to employ the teachings of Hailpern in the virus scanning system of Trcka, Stevens, and Cheriton by modifying mail servers to contain the scanning system of Trcka, Stevens, and Cheriton. This would have been obvious because the ordinary person skilled in the art would have been motivated to enable the proxies to be able to scan the types of communications they already process and therefore reduce network traffic and delay. Further, SMTP mail servers were well known in the art at the time of invention, and it would have been obvious to utilize the scanning system of Trcka and Stevens, and Cheriton in an SMTP mail server. This would have been obvious because the ordinary person skilled in the art would have been motivated to protect SMTP mail servers from viruses.

Claims 53-54 are rejected under 35 U.S.C. 103(a) as being unpatentable over Trcka, Stevens, and Cheriton as applied to claim 32 above, and further in view of Epstein et al. (US Patent Number 6,684,329) hereinafter referred to as Epstein.

Trcka, Stevens, and Cheriton disclosed scanning packets for viruses (See Trcka Col. 11 Lines 1-4), but failed to disclose sub-modules which each scan one of HTTP, FTP, SMTP, and NNTP packets.

Epstein teaches that in a firewall which scans for viruses, proxy sub-modules should be provided in the firewall for each of HTTP, FTP, SMTP, and NNTP protocol packets (See Epstein Col. 1 Lines 27-53 and Col. 3 Lines 8-21).

It would have been obvious to the ordinary person skilled in the art at the time of invention to employ the teachings of Epstein in the virus scanning of Trcka, Stevens, and Cheriton by providing protocol specific proxy servers in the surveillance module to scan each of HTTP, SMTP, FTP, and NNTP packets. This would have been obvious because the ordinary person skilled in the art would have been motivated to provide the network administrator with greater control over the traffic which traversed the network.

Conclusion

Claims 1-10, 13-25, 28-38, 40-47, and 49-55 have been rejected.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew T. Henning whose telephone number is (571) 272-3790. The examiner can normally be reached on M-F 8-4.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

/Matthew Henning/
Assistant Examiner
Art Unit 2131
8/28/2007

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100